Abstract

A stored information protect mechanism related to the field of the computer system and the information security is disclosed. The purpose of it is to provide an efficient method for the computer system with open bus structure. The method is independent of the main CPU and the system software of the system, does not change the system hardware, and be able to avoid the illicit access to the stored information. The technical features of the invention include the protect mechanism based on the level of the circuit signal, the information subscribing registration outside the mechanism, the internal on-line listening, the real-time detection, the fast verification, the leading block and the conversion between these status. The method is very simple and reliable and easy to implement, leading to active effect for resisting the incursion of the computer "virus" and restraining the computer violation.

[19]中华人民共和国专利局

[11]授权公告号
CN 1021089C

[12] 发明专利说明书

[21] 专利号 ZL 90101742

[51]Int.Cl[5]
G06F 12/14

[45]授权公告日 1993年6月2日

[24]颁证日 93.4.16
[21]申请号 90101742.6
[22]申请日 90.4.5
[73]专利权人 杨筑平
地 址 100086 贵州省凯里州人大常委会杨再传收转
[72]发明人 杨筑平 李利安

说明书页数: 附图页数:

[54]发明名称 存储信息保护机构.

[57]摘要

一种存储信息保护机构，属于计算机系统与信息安全领域。目的是为开放性总线结构的计算机系统提供一种有效方法，它独立于系统主 CPU 和系统软件，不更改系统硬件，能够防止对存储信息的非法访问。其特征是基于电路信号一级的保护机制，机构外部信息预约登记，内部在线侦听、实时检测、快速核实、超前封锁及在这些状态间转换运作。本发明方法简练，安全可靠，易于实现，对于抵御计算机"病毒"侵害和抑制计算机犯罪将产生积极效果。

权　利　要　求　书

1.一种存储信息保护方法，其特征是，在计算机系统中连入一个硬件，于外部预约登记待保护信息且登记内容自动受保护，于内部通过系统总线：在线侦听地址，实时检测所访问信息在存储介质上的存储位置和范围，快速核实访问权限，超前封锁非法访问。

2.一种存储信息保护机构，包括地址部件、数据部件、控制部件和固化程序，组成接插件，其特征是还包括总线监控电路，通过总线扩展槽联入计算机系统，能由系统总线上侦测到主 CPU 对存储设备的访问，并可使访问过程延迟或中断。

说　　明　　书

存储信息保护机构

本发明涉及一种存储信息保护机构，属于计算机系统和信息安全领域。

在总线型体系结构的计算机系统尤其是个人计算机系统中，由于系统总线的开放性，存储设备显得十分脆弱——存储信息（程序和数据）很容易被窃取或遭到有意无意的破坏。为了从技术上解决这一问题，人们采取了许多办法，大体分为两类：一是对信息加密（如美国的 DES 标准加密算法），二是限制对信息的访问权限（如计算机局部网络系统中的口令和存取权限功能）。显然，加密仅能相对地对付窃取（“读”操作），却无力对付破坏（“写”操作），因此，限制访问权限乃是根本性的办法。然而，如何有效、可靠地实施限制却又是问题之关键所在。公知的办法（如 Fisher Innis 公司的 WATCHDOG 软件，以及SDI 公司的 STOP LOCKIIR 硬件）是在操作系统的不同层次——外壳、内核或基本 I/O 系统基础上检查和限制对存储信息的访问。但是这些办法的缺陷在于，它们主要依靠在系统主 CPU 上运行相应的软件或程序来完成；而实际上只要使用特别的软件工具，或不同版本甚至不同拷贝的操作系统，就有可能绕过它们的限制直接对存储信息进行访问。因此，这样的方法还不是十分可靠的。迄今为止，尚未有这样的保护机构或方法．它独立于系统主 CPU 和操作系统，既能够可靠地防止对存储信息的非法访问，又不妨碍对存储信息的合法访问。

本发明的目的，是为总线型体系结构的计算机系统提供一种存储信息保护机构，即一种技术方法，它独立于系统主 CPU 和包括操作系统在内的系统软件，且无需更改系统硬件，就能有效地、可靠地防止对存储信息的非法访问，同时又不影响对存储信息的合法访问。

本发明的基本思想，是在原系统硬件环境中附加一个保护机构硬件，尽可能地在系统的最底层堵截对存储信息的非法访问。在功能逻辑上，将保护机构(3)置于读／写伺服机构(2)之上而在读／写控制接口部件(4)之下。于是，用户(6)操纵处理机(5)经读／写控制接口部件(4)，去驱动读／写伺服机构(2)对载有存储信息的物理介质(1)的访问，就必定经过保护机构(3)的过滤。保护机构(3)对于合法访问是透明的．而对于非法访问是不可通过的。

本发明的功能特性，体现在保护机构的外部和内部两个方面。

保护机构的外部应用特性，主要是对所需保护的信息作预约登记。基于具体的计算机系统，机构有两类用户：一个初始的超级用户和若干由超级用户授权产生的普通用户。机构的所有用户通过运行在系统主 CPU 上的一个外部实用程序与机构通信。首先要核对口令，然后可做以下操作：修改口令、登记要保护的信息（文件／扇区／簇／块）、显示受保护信息的记要、指定／修改受保护信息的访问权限（系统、隐含、只读、读／写），以及撤销信息的保护。机构在存储介质上占据若干保留扇区或块，或者采用 MOS 存储器，用以记载全部口令、预约登记，以及必要的系统信息和状态信息。这些保留扇区或块自动受到机构的保护，所采用的 MOS 存储器也只能由机构自己访问。

保护机构的内部系统特性，包括在线侦听、实时检测、快速核实和超前封锁。机构内部工作过程可借助状态转换图来描述。机构通过地址部件(2)，始终处于侦听状态；当且仅当从地址总线上发现系统有对存储设备的访问时，便进入检测状态。机构通过数据部件(1)，根据从数据总线上截取的即将访问存储设备的存储介质之位置和范围（柱面、磁头、扇区、块）诸元，判断当前访问是否涉及已登记保护的信息；若是无关访问则返回侦听状态，若是相关访问则进入核实状态。机构通过控制部件(3)和数据部件(1)，根据从控制总线和数据总线上获知的访问操作（读，写，格式化等），参照已登记保护之信息的访问权限，核查是否合法访问；是则返回侦听状态，否则进入封锁状态。机构针对非法访问，由控制部件(3)经系统总线迅速强制予以封锁，使其失效；同时显示错误信息，发出声音报警，以及自动记录非法访问事件。封锁完毕，返回侦听状态。

本发明的可行性，建立在总线结构的开放性之基础上。亦即，保护机构可与总线上其他设备或部件同样平等地连入和使用系统总线。同时，保护机构的运作与系统主 CPU 是并行的，且独立于后者。保护机构的封锁机制，是对读／写存储设备之电路信号在时序上的干扰与剥夺。

本发明与现有技术相比，具有明显优点：一是方法简炼，思路清晰，体系完整；二是基于电路信号一级的保护机制，更加安全可靠；三是独立于具体的计算机系统，

便于开发实现。本发明的实施与应用，对于抵御计算机“病毒”侵袭危害和抑制计算机犯罪，提供了一种强有力的技术手段并将产生积极的效果。对于开放性总线体系结构的计算机系统尤其是个人计算机系统，本发明及其实现产品具有普遍的实用价值。

图 1 表达本发明在计算机系统中的功能逻辑关系。图中，1为物理介质及存储信息，2为读／写伺服机构，3为保护机构，4为读／写控制接口部件，5为处理机，6为用户。

图 2 是保护机构内部工作过程状态转换图。其中，“侦听”既是初态又是终态。

图 3 表明保护机构的内部构成。图中，1为数据部件，2为地址部件，3为控制部件，4为 CPU，5为随机存取存储器，6为只读存储器，7为时钟发生器，8为 MOS 存储器，9为电池。其中，8和9可以为空。

下面结合图三说明实现本发明的一种最佳方案。

保护机构作为一个实体，以总线接插件形式实施。其中，

1）地址部件(2)包括一个地址缓冲器，一个地址寄存器和一个与门。缓冲器接收到的地址与寄存器中已由 CPU (4)预置的存储设备之地址，经与门相“与”，其结果按正逻辑，作为激活“检测”状态并开启数据部件(1)和控制部件(3)的条件。

2）数据部件(1)包括一个双向数据锁存器。

3）控制部件(3)与系统控制总线对应相容。

4）CPU (4)采用 INTELL 8088。

5）随机存取存储器(5)采用静态 RAM，以省去刷新电路和提高存取速度。

6）只读存储器(6)采用一片 27256。

7）时钟发生器(7)自备，以便机构与系统主 CPU 独立且并行。

8）MOS 电路(8)采用低功耗的 CMOS 器件。

9）电池(9)采用6V可充电电池，用以保持 CMOS 中所存信息。充电电源经由系统总线取自主机板。

专利号 90 1 01742
Int. Cl.[5] G06F 12/14
授权公告日 1993年6月2日

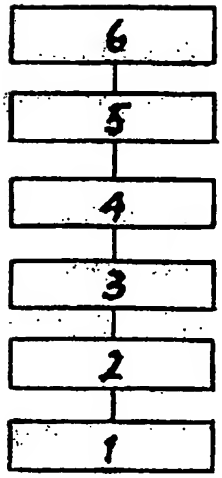

图 1

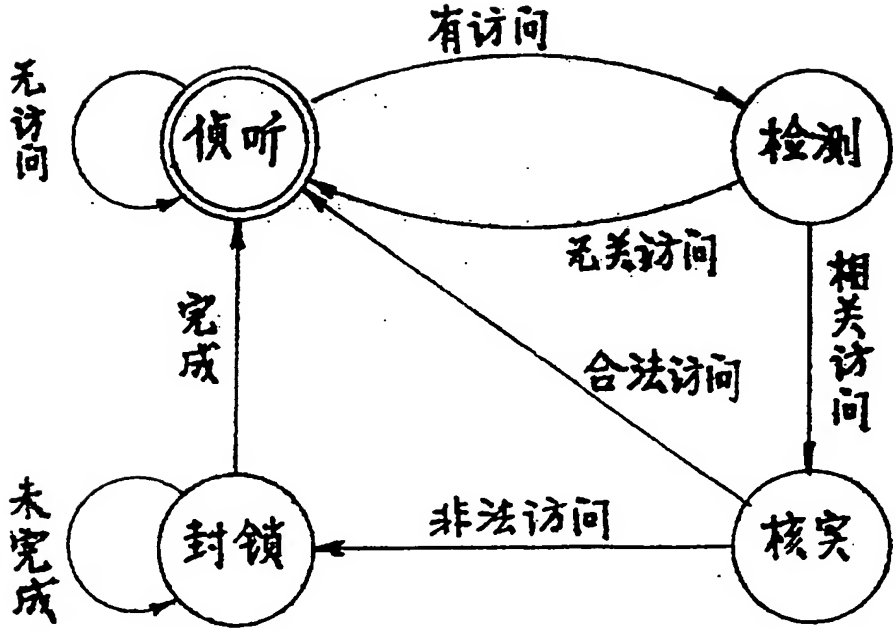

图 2

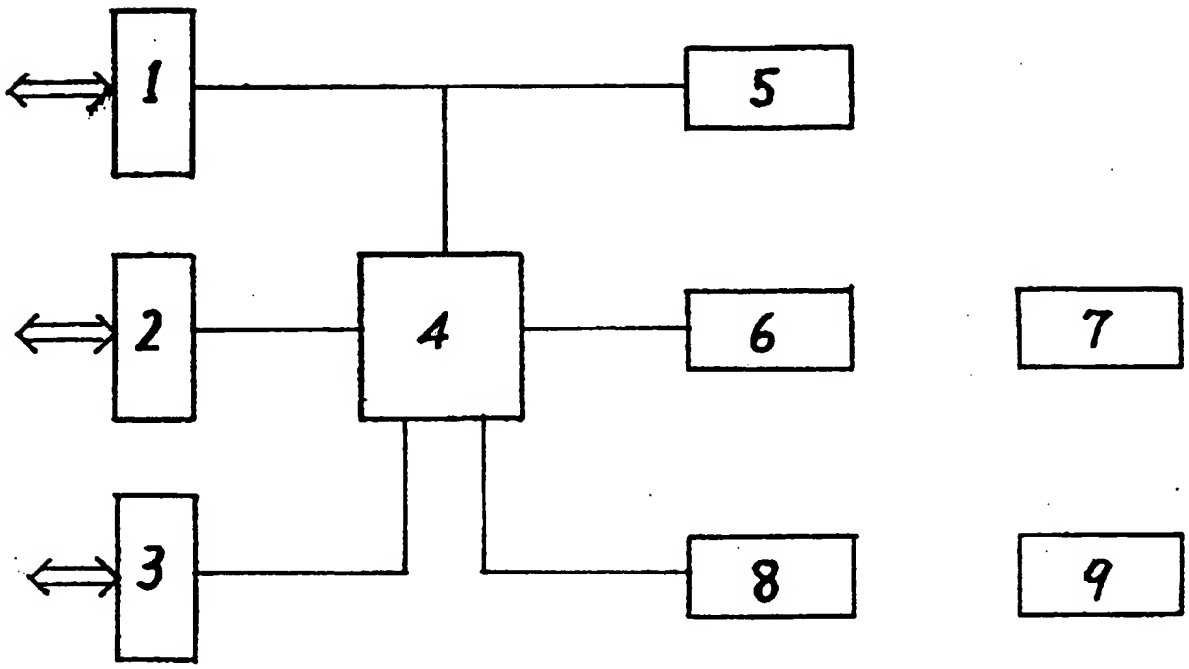

图 3